IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEBRASKA

UNITED STATES OF AMERICA, Plaintiff, vs. RYAN KEITER, Defendant.	**4:13CR3004** **FINDINGS, RECOMMENDATION, AND ORDER**

This matter is before the court on defendant Ryan Keiter's motion to suppress evidence and request for an evidentiary hearing, (Filing No. 13). For the reasons set forth below Keiter's motion should be denied in its entirety.

BACKGROUND

On February 27, 2012 a Federal Bureau of Investigation ("FBI") agent in Los Angeles, California used a file sharing program called Gigatribe to download images depicting child pornography. Those images included the following:

> pict1435.jpg- This is an image of a seven to nine year old naked white female. The image shows a seven to nine year old white female's legs and waist tied to a chair with white rope. An adult white male's left index finger is inserted in the seven to nine year old white female's vagina. The seven to nine year old white female is wearing a purple wrist watch on her right arm. The focal point of this image is on the seven to nine year old white female's vagina.
>
> 1171040106801.jpg- This is an image of a nine to eleven year old naked white female on a bed as she is kneeling down and leaning forward on her elbows. The nine to eleven year old white female's arms are tied to the head board of the bed with white rope. The nine to eleven year old white female has a purple sex toy inserted in her vaginal and anal area.
>
> img20040907092218.jpg - This is an image of a four to six year old naked

> female laying on her back on a pillow. The four to six year old female's legs are spread to expose the four to six year old female's vagina. An adult female is holding a sex toy near the four to six year old female's vagina. The four to six year old female's vagina appears to be illuminated by an extra light source.

(Filing No. 22-1, at CM/ECF pp. 20-21).

The shared files were downloaded from the computer of an individual with the username "Johnny_Rocker" utilizing a computer with the Internet Protocol ("IP") address[1] 76.84.42.205. FBI agents determined the IP address in question was registered to Time Warner Communications and assigned to an account at 2358 South 27th Street, Lincoln, Nebraska.

FBI agents obtained and executed a search warrant for 2358 South 27th Street residence on April 13, 2012. During the execution of the warrant the agents conducted a "forensic preview" of the computers in the home and found that none of the computers contained child pornography or peer to peer ("P2P") software.[2] The owner of the residence stated that his home's wireless internet connection was not secured or

[1] "The Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses while other computers have dynamic—that is, frequently changed—IP addresses." 113 Am. Jur. Proof of Facts 3d 1 (Originally published in 2010).

[2] As explained by Agent Sara Kane's application for search warrant, "Peer-to-peer file-sharing" (P2P) is a method of communication available to Internet users through the use of special software. Computers linked together through the Internet using this software form a network that allows for the sharing of digital files between users on the network. A user first obtains the P2P software, which can be downloaded from the Internet. In general, P2P software allows the user to set up files on a computer to be shared with others running compatible P2P software. A user obtains files by opening the P2P software on the user's computer, and conducting searches for files that are currently being shared on another user's computer." (Filing No. 22-1, at CM/ECF 10).

encrypted. The FBI investigators accessed the administrative section of the home owner's wireless access point and determined the home owner's wireless internet had been accessed by two foreign devices – that is, devices that did not belong to the home owner. Those two devices were listed as "Ryan-IPad" and "Ryan-HP."

During the execution of the search warrant on the house at 2358 South 27th Street, one of the members of the FBI's investigation team, Special Agent Sara Kane, observed a 1999 Pontiac Grand Prix parked in the driveway to the residence next door – 2352 South 27th Street. A records check revealed that vehicle belonged to the defendant, Ryan Keiter.[3]

At approximately 7:50 a.m. that same morning, investigators knocked on the door of 2352 South 27th Street. Investigator Scott Haugaard of the Nebraska State Patrol knocked on the back door and was greeted by Keiter. Haugaard asked Keiter if they could talk inside Keiter's home. Keiter declined to allow Haugaard to enter the residence, but engaged in a conversation with Haugaard. Haugaard informed Keiter that he was not required to talk with Haugaard and that Keiter was free to leave at any time.

Keiter admitted that he did not have an internet connection originating from his residence, but accessed a wireless connection of which he claimed he did not know the owner. When asked about whether he knew anything about child pornography, Keiter initially denied having any such knowledge. Haugaard informed Keiter that the law enforcement officers intended to secure the residence and "get a search warrant to search your residence." (Filing No. 17-1, at CM/ECF p. 4). Haugaard continued to ask Keiter questions about Keiter accessing child pornography and the following exchange occurred:

[3] The vehicle registration reflected an address of 413 Fletcher Ave, Apt. 12, Lincoln, Nebraska. Keiter confirmed that he had been living at the 2352 South 27th Street for approximately 4 months. Filing No. 17-1, at CM/ECF p. 7.

Haugaard: How long have you been doing child porn?

Keiter: I don't want to say anything because I don't . . .

Haugaard: Okay.

Keiter: I'm not admitting anything for right now.

(Filing No. 17-1, at CM/ECF p. 6).

Agent Haugaard also asked Keiter if he used the internet username Johnny_Rocket which led to the following exchange:

Haugaard: I can't give you advice, I can't coax you, I can't you know, coerce you, okay? I would much rather not go down that road, okay? You'd be much better off just not answering that question just like you have been, okay? Are you Johnny underscore Rocket?

Keiter: I don't know.

Haugaard: Is that a no or an I don't wanna' talk about it?

Keiter: I don't want to say anything 'cause I don't wanna' lie . . . .

(Filing No. 17-1, at CM/ECF p. 17).

Keiter further stated that he owned a laptop and an iPad and that he had used "peer programs like Bearshare, Frostwire, [and] Limewire . . .in the past" although he denied using Gigatribe. (Filing No. 17-1, at CM/ECF p. 9). In response to the officer's questioning, Keiter stated he did not know why he used P2P programs, but they were not

being used for viewing or receiving child pornography. (Filing No. 17-1, at CM/ECF p. 10).

Keiter asked law enforcement officers if he could change clothes and leave for work. Haugaard informed Keiter that law enforcement officials were going to "secure" the house and that Keiter would be allowed to change clothes, but only after the investigators made sure the house was secure. The officer's also advised Keiter that he was not under arrest and he was free to leave.

> Keiter: Well, I need to, like, get ready for work and stuff, what is your process right now?
>
> Haugaard: Our process is going to be that we are going to dominate this house, we are going to secure it, we're going to contact the judge and ask for authorization to, uh, search your residence and seize computer media associated with the possession and distribution of child pornography. . . . So, the process being we're gonna' sit here until we get, uh, the piece of paper that says I can search your residence. . . .

(Filing No. 17-1, at CM/ECF p. 10).

. . .

> Haugaard: We are going to wait until we get a piece of paper, and then we are going to search your house, okay? We're letting you come back inside so that you can get dressed and we don't put too much of a damper on the business life of yours, okay? You're not under arrest and you're free to leave. . . .

(Filing No. 17-1 at CM/ECF p. 11).

> Keiter: So, I'm just supposed to allow you guys to be here? Is that what you are saying?

> Haugaard: You don't have a choice. I allowed you to get dressed. As soon as you leave, my threat is gone, okay? And then we're gonna' step outside and we're gonna' wait for a piece of paper so we can search your house, okay?

(Filing No. 17-1, at CM/ECF at 14).

Keiter was further informed that although he was free to leave, he would not be able to take some of his property, including his electronics and his car, unless the investigators could make certain his car did not contain any computers. He consented to the search of his car and left for work. A search warrant was drafted by Agent Sara Kane and presented to the undersigned Magistrate Judge on April 13, 2012. The warrant was issued, and it was executed later that day.

The warrant stated that based upon her training and experience in child pornography investigations, Agent Kane knows that persons who distribute, transport, receive, or possess child pornography maintain copies of the child-pornography materials in the privacy and security of their home or some other secure location. Even if child pornography collectors choose to "delete" a file from a computer, the data contained in the file does not actually disappear; rather, the data remains on the hard drive until it is overwritten by new data.

In addition to general information about P2P software and the characteristics of child pornography collectors, the warrant provided specific information about the investigation, including the circumstances surrounding the execution of the original warrant, the information regarding Keiter's admission of his unauthorized use of his neighbor's wireless internet with his HP laptop computer and his iPad, Keiter's admission that he had previously used P2P software, and Keiter's response that he did not want to answer a question about child pornography or whether he used the username

Johnny_Rocker.[4] (Filing No. 22-1, at CM/ECF p. 22-23). The affidavit further represented that Keiter was informed that law enforcement officers intended "to secure his residence in anticipation of obtaining a search warrant for his residence." (Filing No. 22-1, at CM/ECF p. 23). Keiter now contests the validity of the search warrant and seeks to suppress evidence obtained as a result of the search.

LEGAL ANALYSIS

Keiter argues the evidence against him should be suppressed for several reasons. First, he contends the search warrant was not supported by probable cause. Second, he asserts the information contained in the warrant was stale. Finally, he argues that Kane intentionally, knowingly or recklessly omitted facts from her affidavit which, had those facts been included, would have negated a finding of probable cause. Accordingly, he seeks a hearing pursuant to Franks v. Delaware, 438 U.S. 154 (1978). Each argument is addressed in turn below.

Probable Cause for Warrant.

A warrant application must be submitted to a neutral, detached judicial officer for a determination of whether "there is probable cause to believe evidence, instrumentalities, or fruits of a crime, [or] contraband . . . may be found in the place to be searched." United States v. Houston, 754 F. Supp. 2d 1059, 1073 (D.S.D. 2010)(citing Walden v. Caramak, 156 F.3d 861, 870 (8th Cir. 1998).

> "To determine whether probable cause exists to support a search warrant we look at the 'totality of the circumstances.' " United States v. Reinholz,

[4] It appears from the transcripts that Inv. Haugaard asked Keiter if he used the username "Johnny_Rocket" while the affidavit provides the username under investigation was "Johnny_Rocker."

> 245 F.3d 765, 776 (8th Cir.2001) (quoting Illinois v. Gates, 462 U.S. 213, 230, 234, 103 S.Ct. 2317, 76 L.Ed.2d 527 (1983)). "A warrant is supported by probable cause if there is a fair probability that contraband or evidence of a crime will be found in the place to be searched." Id. (quotation and citation omitted). "We assess probable cause from the viewpoint of a reasonably prudent police officer acting in the circumstances of the particular case." Id. (internal citations omitted). "[P]robable cause is a practical, factual, and nontechnical concept, dealing with probabilities." Id. "The determination of whether or not probable cause exists to issue a search warrant is to be based upon a common-sense reading of the entire affidavit." United States v. Sumpter, 669 F.2d 1215, 1218 (8th Cir.1982) (quotation and citation omitted).

United States v. Seidel, 677 F.3d 334, 337-38 (8th Cir. 2012).

When the judicial officer issuing the search warrant relies entirely upon a supporting affidavit of a law enforcement officer, "only that information which is found within the four corners of the affidavit may be considered in determining the existence of probable cause." United States v. Solomon, 432 F.3d 824, 827 (8th Cir. 2005)(citations omitted). The judicial officer uses "common sense approach" when examining the affidavit, and does not scrutinize it "in a hypertechnical fashion." United States v. Williams, 10 F.3d 590, 593 (8th Cir. 1993). The issuing judge may consider observations made by trained law enforcement officers as one factor in his or her probable cause determination. Walden, 156 F.3d at 870 (citations omitted).

Keiter asserts the warrant is unsupported by probable cause on its face. Keiter points to several alleged deficiencies in the affidavit to support his claim. Specifically, he argues the warrant did not indicate "how many devices were connected to the wireless access point, when they were connected to the wireless access point, [] which devices were connected to the wireless access point when the alleged pornography was downloaded" by the FBI, . . . [and] failed to provide any verification that the Ryan I-Pad and the Ryan-HP were connected to the wireless access point . . . on or about the time the

crime was committed." (Filing No. 14, at CM/ECF p. 5). Further, Keiter argues the affidavit was deficient because it did not specify whether IP address 76.84.42.205 was static or dynamic.[5]

The court finds no merit to Keiter's assertion that the "missing" information was essential for a finding of probable cause. The affidavit contained ample evidence to support a finding of probable cause. Law enforcement agents knew someone with devices named "Ryan I-Pad" and "Ryan-HP" were connecting to the wireless access point without prior authorization. It was determined that Keiter kept computers in his house; was the next door neighbor to the home containing the wireless internet access point; lived at his residence during the time period when agents discovered the downloaded child pornography; used his neighbor's wireless internet service without permission; had previously used P2P software; and refused to answer questions about whether he downloaded child pornography from the internet.[6] This information which was included in the Kane's affidavit in support of the warrant application was more than sufficient to support the conclusion there was "a fair probability that contraband or evidence of criminal activity [would] be found" in Keiter's electronic devices. Mutchelknaus, 592 F.3d at 828.

While the court has determined the face of the warrant and supporting affidavit contained sufficient information for a finding of probable cause, Keiter's concerns regarding whether the IP address was static or dynamic warrant specific mention.

---

[5] As explained by Keiter, a static IP address "means that a computer with an assigned IP address uses the same IP address when connecting to the internet," whereas a dynamic IP address "changes each time a device logs in to a network." (Filing No. 14, at CM/ECF p. 6 (citations omitted)).

[6] The affidavit also disclosed that Keiter did not want to answer the question as to whether his user name was "Johnny_Rocker." As noted above, Keiter was actually asked whether he used the name "Johnny_Rocket." This error is of no consequence as the court finds there was sufficient information in the affidavit for a finding of probable cause even without the question regarding the username.

Whether the IP address in question was static or dynamic is simply not relevant. Keiter argues that "[i]f the address was dynamic, law enforcement would need to do more to pin the specific download of child pornography on a device at 2358 South 27th Street." Keiter provides little else by way of explanation as to how this information was relevant, particularly since the investigators were certain that the IP address in question had been assigned to the house on South 27th Street at the time the child pornography was downloaded. That is, law enforcement officers were certain at the time relevant to the warrant, someone using a computer with the wireless access point at 2358 South 27th Street – i.e., a computer using the IP address in question – downloaded child pornography using P2P software.

Stale information.

Stale information cannot be considered when assessing probable cause. "Probable cause must exist when a warrant is issued, not merely at some earlier time. . . ." United States v. Morrison, 594 F.3d 626, 631 (8th Cir. 2010). There is no bright line test for determining when information is stale. The court must consider time factors in the context of a specific case and the nature of the crime under investigation. "The lapse of time is least important when the suspected criminal activity is continuing in nature and when the property is not likely to be destroyed or dissipated." United States v. Lemon, 590 F.3d 612, 614 (8th Cir. 2010). "Possession of child pornography is a crime that is continuing in nature." Lemon, 590 F.3d at 614. When investigating ongoing criminal activity, intervals of weeks, months, or even years between the last described act and the application for a warrant does not necessarily make the information stale. Morrison, 594 F.3d at 631; Lemon, 590 F.3d at 614.

In this case, an FBI agent originally accessed the downloaded files allegedly depicting child pornography from a computer accessing the wireless internet at 2358 S.

27th Street on February 27, 2012. The search warrant on Keiter's residence was executed on April 13, 2012, a mere 46 days later.

As set forth in Agent Cane's warrant affidavit, those who collect child pornography tend to keep their files nearby and for extensive time periods, and even if they attempt to delete a file, the file remains on the computer until the space is overwritten – i.e., a potentially indefinite period of time. See Lemon 590 F.3d at 614. Further, she explained that child pornography collectors often maintain their files in their residence. Based on the totality of facts in the warrant affidavit, the information obtained by law enforcement agents less than two months earlier was not stale. Lemon, 590 F.3d at 614 (holding evidence of child pornography located 18 months earlier was not stale where the officer stated the IP address and screen name were still being used, and based on the officer's training and experience, he explained that collectors of child pornography maintain their collections for a long period of time); see also United States v. Estey, 595 F.3d 836, 840 (8th Cir. 2101)(five month delay after child pornography evidence was discovered did not render information stale).

Franks hearing.

Under Franks v. Delaware, 438 U.S. 154 (1978), a defendant is not entitled to a hearing on his claim that the affiant officer intentionally or recklessly misstated or excluded material information from a warrant application unless the defendant first shows that the warrant application, corrected to remove allegedly false information and include allegedly concealed facts, would not have supported a finding of probable cause. Franks, 438 U.S. at 170; United States v. Frazier, 280 F.3d 835, 845 (8th Cir. 2002).

> We apply a two-part test to allegations of omissions of fact in violation of Franks, requiring the defendant to show that the affiant omitted facts with the intent to make, or in reckless disregard of whether the omissions made,

> the affidavit misleading, and that the affidavit, if supplemented by the omitted information, could not support a finding of probable cause.

United States v. LaMorie, 100 F.3d 547, 555 (8th Cir. 1996).

Stated another way, in order to qualify for a Franks hearing, the defendant must meet two criteria. First, the defendant bears the burden of establishing by a preponderance of the evidence that the affiant knowingly and intentionally, or with reckless disregard for the truth, omitted facts from, or included false statements in, the affidavit. United States v. Williams, 981 F.2d 1003, 1005 (8th Cir. 1992). Second, the defendant must show that either the alleged omissions were necessary to a finding of probable cause or that if the false statements are "set aside the affidavit's remaining content is insufficient for a finding of probable cause." Williams, 981 F.2d at 1003; LaMorie, 100 F.3d at 555. If the defendant is not able to satisfy both of these requirements, he is not entitled to a Franks hearing. United States v. Stropes, 387 F.3d 766, 771 (8th Cir. 2004). "The type of showing required [for a Franks hearing] is not easily met." United States v. Gabrio, 295 F.3d 880, 883 (8th Cir. 2002).

Keiter argues he is entitled to a Franks hearing because the affidavit presented to the undersigned did not disclose that six law enforcement officers entered Keiter's residence without his permission, "searched" his home, and did not find a laptop or an iPad. In support of his assertion, Keiter submits an affidavit in which he states: "I believe based on sounds and voices created by other officers, that my house was being searched." (Filing No. 17-1 p. 20).

As an initial matter, Keiter has not met his burden of proving Kane knowingly and intentionally omitted, or recklessly disregarded, the fact that the officers entered the home and secured it in anticipation of receiving a search warrant. The affidavit notified the undersigned magistrate judge that Keiter was informed his house would be secured while

the law enforcement officers waited for a warrant. (Filing No. 22-1, at CM/ECF p. 23). Although Keiter states it sounded like his house was being searched and not just secured,[7] Keiter's statement of alleged officer misconduct is, at most, speculative. Keiter has provided insufficient evidence to meet his burden that the house was searched before the warrant was obtained or that Kane knowingly and intentionally omitted, or recklessly disregarded, that fact.

Further, Keiter's assertion that the house was searched by law enforcement officers is contradicted by the actual transcript of the encounter with Keiter. The transcript makes clear that law enforcement officers consistently told Keiter the house would be secured, but that they would wait for a search warrant to conduct the actual search. In fact, the officers told Keiter that once Keiter left for work, the officer's would wait outside the home until they obtained a court-issued search warrant. It is clear from the evidence that while the officers may have secured the home, they had no intention of conducting a warrantless search of the house or any electronic devices.

Finally, even had Kane's affidavit specifically stated that the officers entered and secured Keiter's residence, those facts would not have been material to the finding of probable cause. Aside from Keiter's speculation, there is nothing to indicate the officers exploited their presence in the home by looking for or conducting forensic examinations on computer equipment. Thus, even if Kane had specifically included in her warrant that officers entered Keiter's house and secured it while Keiter changed clothes, a finding of probable cause undoubtedly would have been made.

In short Keiter has not met his burden of proving that Kane intentionally, knowingly, or with reckless disregard omitted facts from her affidavit. And even if the

[7] Law enforcement officers are, on the basis of probable cause, entitled to secure a residence to prevent the destruction or removal of evidence while a search warrant is being sought. United States v. Ruiz-Estrada, 312 F.3d 398, 404 (8th Cir. 2002).

alleged omissions are now included and considered, the warrant still supports a finding of probable cause. Accordingly, Keiter is not entitled to a Franks hearing.

IT THEREFORE HEREBY IS RECOMMENDED to the Honorable Richard G. Kopf, United States District Judge, pursuant to 28 U.S.C. § 636(b), that the motion to suppress and request for an evidentiary hearing filed by, Ryan Keiter, (Filing no. 13), be denied in all respects.

The parties are notified that failing to file an objection to this recommendation as provided in the local rules of this court may be held to be a waiver of any right to appeal the court's adoption of the recommendation.

IT IS FURTHER ORDERED, the trial of this case is set to commence before the Honorable Richard G. Kopf at 9:00 a.m. on June 3, 2013, or as soon thereafter as the case may be called, for a duration of four (4) trial days, in Courtroom 1, United States Courthouse, Lincoln, Nebraska. Jury selection will be held at commencement of trial.

Dated this 29th day of April, 2013.

BY THE COURT:

s/ Cheryl R. Zwart
United States Magistrate Judge